ABSTRACT

A processor having a general-purpose function and a security dedicated function (i.e., safe keeping of key data and high-speed digital signature calculation) is provided. Key data is stored in a non-volatile key register 130 of a secure processor 100, which has general instructions and signature calculation instructions. A key bit reference counter 152 decreases by one from 1023 to 0 sequentially. In conformity with the content of this key bit reference counter 152, a bit designating gate 154 designates k data stored in the non-volatile key register 130 bit by bit, which is then used for sequential signature calculation. A word data parallel transmission path, which allows data to be transferred from the key register 130 to others, is not provided. With such a hardware structure, it is impossible to directly output raw key data to the outside.